SOLUTION BRIEF

Securing On-Premise Environments with Armis for DoD

Executive Summary

The Department of Defense (DoD) faces mounting cybersecurity risks from adversarial nation states across the enterprise. As adversaries grow more sophisticated, traditional cyber security solutions fall short in providing the complete visibility, security and control necessary to secure IT environments. Armis delivers a purpose-built, on-premises Cyber Asset Attack Surface Management (CAASM) solution designed to empower the Defense Department with comprehensive cyber exposure management, asset discovery, and vulnerability prioritization & mitigation solution, without compromising operational continuity or data sovereignty.

The Challenge

On-Premise environments have long served as the preferred architecture in safeguarding national security assets by isolating critical systems from the internet and broader networks. Unfortunately, isolation alone is not impenetrable. Insider threats, removable media, and legacy systems expose these environments to potential intrusions, lateral movement and ultimately operational disruption.

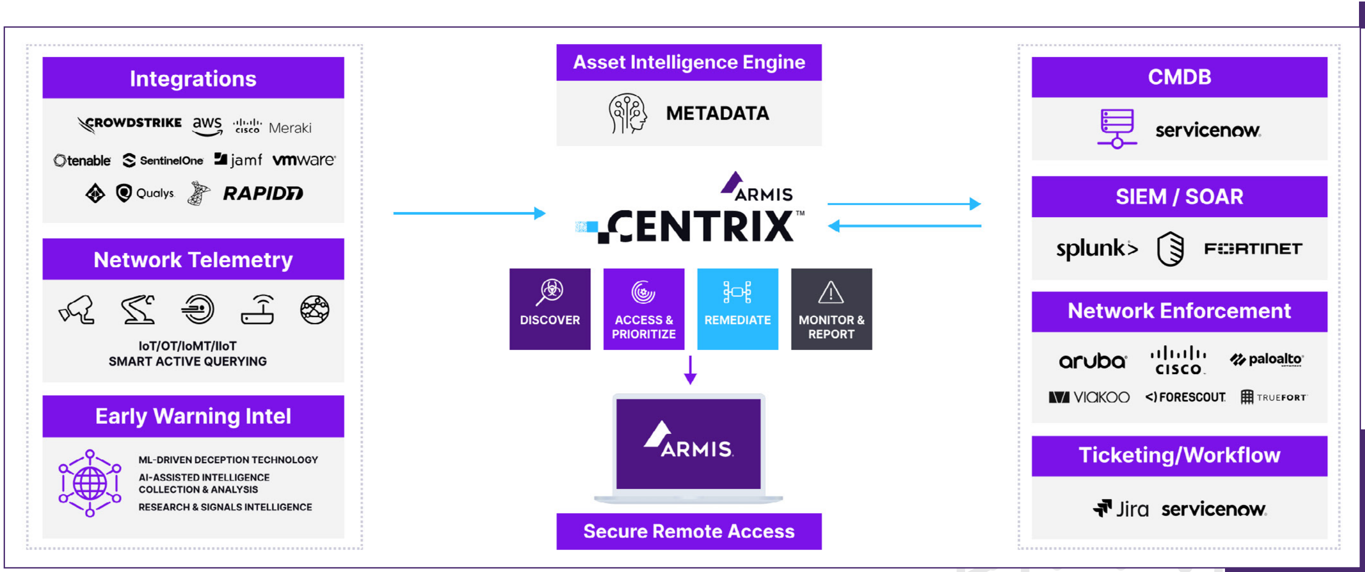
Key challenges include

> **Limited Visibility:** Legacy security tools fail to uncover unmanaged, ephemeral or undocumented IT and cyber-physical assets.

> **Stagnant Vulnerability Management:** On-Premise systems often fall behind in patch management and fail to detect evolving threats.

> **Inconsistent Security Posture:** Despite investments in on-premise GOTS & COTS solutions, these capabilities often operate independent of each other. Integration has proven challenging, cost prohibitive, and traditionally reactive as opposed to proactive.

Federal agencies require a modern, stable, and secure platform that thrives within these constraints which is why **Armis On-Premise** was developed.



Introducing Armis for On-Prem Environments

Armis On-Premise is the definitive solution for cyber exposure management and security in on-premise, classified, environments. It brings DoD organizations unparalleled visibility to the ecosystem of connected devices, empowering defensive cyber operators to secure critical IT infrastructure and mission systems with autonomy, speed, and resilience.

Key Benefits

- **Unrivaled Stability:** Hardened and optimized for isolated and high-security environments.
- **Comprehensive Asset Discovery:** Discover, classify, and continuously monitor IT, other connected assets locally.
- **Advanced Gap & Vulnerability Analysis:** Identify misconfigurations, risks, and potential attack vectors throughout your IT enterprise including device, assets, network, etc.
- **Zero Trust for Disconnected Networks:** Enforce granular identity-based policies, isolate anomalies, perform real time observability and facilitate STIG baseline analysis within your environment.*
- **Operational Continuity:** Maintain mission assurance with a platform engineered for uninterrupted service in the most sensitive networks.
- **Mobility & Tactical Edge:** Rapid deployment ready via a minimum container footprint, enabling forward deployed mission sets or Fly-away-kit integration.

Purpose-Built Capabilities To Enable Mission Outcomes

Armis On-Premise is the definitive solution for cyber exposure management and security in on-premise, classified, environments. It brings DoD organizations unparalleled visibility to the ecosystem of connected devices, empowering defensive cyber operators to secure critical IT infrastructure and mission systems with autonomy, speed, and resilience.

* currently in development

Infrastructure Asset Discovery

Armis On-Premise enables complete visibility into every connected device, managed or unmanaged, and across your entire IT environment. identifying technical gaps through the continuous collection, profiling, and fingerprinting of assets. A comprehensive understanding of the complete attack surface is achieved through strategic technological integrations and passive network detection with existing on-premise tools and infrastructure.

Vulnerability Identification & Management

Armis aggregates vulnerability insights via multi-detection data collection, strategic integrations, and correlates threat intelligence feeds*, CVEs*, and behavior-based indicators to prioritize remediation efforts. Capabilities include:

> **Risk Contextualization:** Prioritize vulnerabilities, and risk findings, based on asset criticality, operational impact, and network segmentation models.

> **Early Warning Detection:** Leverage AI and deception technology, Armis finds attacks and adversary TTPs to stop attacks while still in the formulation stage.*

Secure Supply Chain Risk Management*

The modern supply chain introduces a complex array of cybersecurity challenges, from counterfeit components to tampered firmware. Armis On-Premise enables federal agencies in maintaining a secure and trusted supply chain across their IT footprint. by continuously auditing and cross referencing your current product ecosystem against product banned lists, End of life hardware & software lists, manufacturer operating system end of service notices, deployed counterfeit hardware, and defunct firmware versions.

> **Anomaly Detection:** with Armis asset profiling, defensive cyber operators are able to audit and cross reference their IT ecosystem against product banned lists, end of life hardware & software notices, manufacturer operating system end of service notices, deployed counterfeit hardware, and defunct firmware versions.

> **Behavioral Monitoring:** Armis tracks how devices behave on the network. It detects malicious firmware activities, unauthorized communications to foreign or untrusted IP addresses, and behavioral anomalies that suggest supply chain compromise.

With Armis On-Premise, the Defense Department will be able to extend Zero Trust principles into the supply chain, validating every device’s origin, integrity, and function.

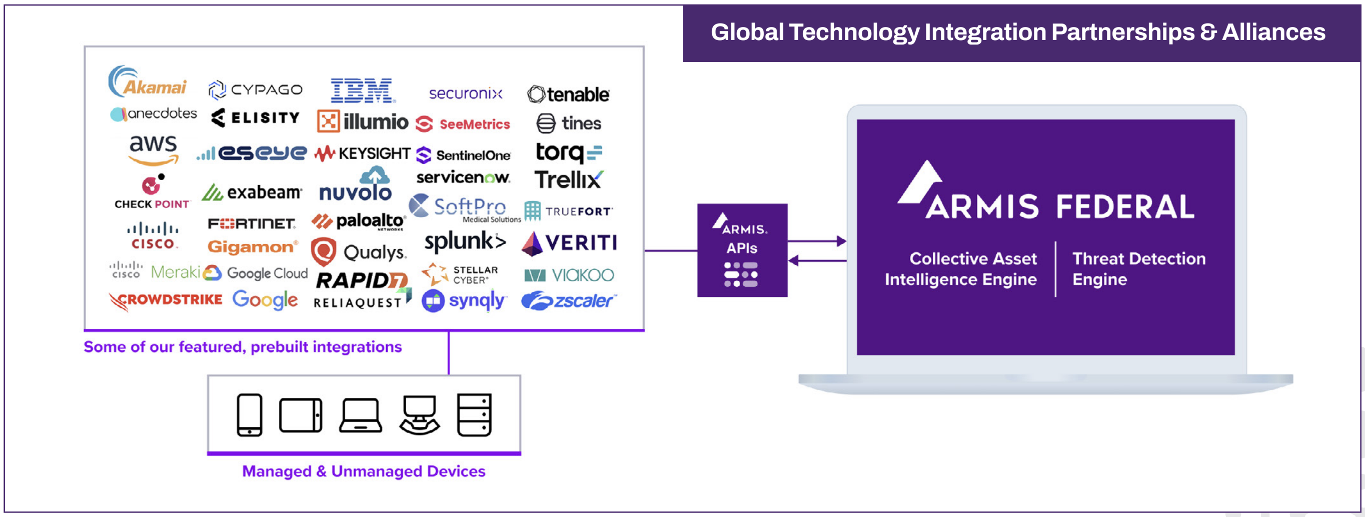
* currently in development

Network Policy Enforcement and Segmentation

Segmentation is a core pillar of modern cybersecurity architecture and is essential to upholding Zero Trust principles. Armis enhances network segmentation and policy enforcement by providing deep visibility into communication flows and boundary enforcement.

> **Zero Trust Microsegmentation:** port, protocol, and communication zone enforcement, enabling the implementation of automated security policies Armis dynamically maps inter-asset communications and helps enforce logical segmentation within your IT environment.

> **Policy Violation Alerts:** Armis identifies and alerts on communications that violate established policies, such as unexpected device-to-device traffic, defunct protocol usage, or connections over prohibited ports. This ensures continuous enforcement of security policies and allows agencies to quickly contain unauthorized behavior before it escalates.



Mobility & Tactical Edge: Armis On-Premise Fly-Away Kit

For forward deployed operations in contested, disconnected, environments, Armis On-Premise includes everything required to develop an isolated asset observability platform for Fly-Away Kit integration, such as:

- Autonomous operation with full localized observability.
- Asset discovery and deep situational awareness.
- Multi detection engine discovery methodologies
- Vulnerability detection and prioritization
- Risk & threat insights to connect the finding to the fix
- Proactive defense and incident response without reliance on external infrastructure

Conclusion: Visibility is Security

On-Premise environments provide isolation, but not immunity. Armis On-Premise brings the Department the next-generation on-premises CAASM platform to bridge visibility gaps, enforce Zero Trust, and secure defense infrastructure with confidence even in the most challenging, mission-critical settings.

With Armis, no asset is left unseen, no vulnerability remains hidden, and no threat goes unchallenged.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo